House Permanent Select Committee on Intelligence
Open Hearing
Written Testimony for the Record

February 2, 2005

Michael S. Swetnam
CEO & Chairman
Potomac Institute for Policy Studies

I would like to thank the Chairman, Congressman Hoekstra and the Ranking Member Congresswoman Harmon for inviting me to testify today and also for their enlightened leadership this past year in helping to create and shepherd through the Intelligence Reform Act. This landmark law is a significant and meaningful start in our efforts to create an intelligence apparatus that will protect America in the decades to come.

I would also like to commend the Chairman and Ranking Member for focusing this years Congressional session on the threat and how best to address it. In reality, even with Al-Qaeda being pursued, threats to our national security are growing. We must address these threats sooner rather than later. We must expand our ability to identify and locate with precision individuals who pose a great threat, greatly strengthen our ability to prevent technological surprise in areas like bio, neuro and nano technology-perhaps create a DARPA for the intel community; bring massive new sensor, modeling and automation to bear on our analytic processes; improve our humint and cultural intelligence, and across the board emphasize knowledge over data. These actions will not be free, but this is essential investment for our nation. This Committee, the Congress and the President have given us smart legislation; now we need focus on smart policy and adept execution to give that legislation full effect.

The Threat

Today the United States and indeed the free world, faces a myriad of threats that were almost inconceivable only a decade ago. We continue to be threatened by large nation states that are coming into their own economically and whose military might is growing at a rapid pace. Regional powers such as China will certainly challenge us economically, and increasingly militarily as their might and influence grows. Similarly, we must continue to watch closely rogue actors like N. Korea, regions that lack effective governance, and the still reforming former Russian states. These fledgling democracies have not matured to the point where a future of democracy is guaranteed. Nor are they fully partners in world peace. We must continue to be very vigilant and watchful as they mature.

But the most frightening threats of this new century are posed not by nation-states, but by increasingly militant individuals and small groups capable of inflicting catastrophic damage on our nation, its economy, and our society. There have always been radical individuals and groups who sought harm to peace loving societies. Human history is full of examples and events perpetrated by individuals and groups that disrupted the peace and security of society. The difference today is technology, specifically the spread of advanced and emerging technology, can be used to cause overwhelming damage and death.

The later part of the last century was uniquely characterized by the threat of thermo-nuclear war. The technology of nuclear weapons completely changed the consequences and prospects for war and peace. Our national security strategy was designed to counter the spread of nuclear weapons technology and to balance international power and influence with those who held this power. We were largely successful with this strategy because we were able to limit the spread of the technology as well as limit access to materials necessary to construct a weapon. Today, we are finding it increasingly difficult to control the spread of technology. Modern communications technologies such as the internet make it almost impossible to prevent the spread of knowledge about any technology. We are still able to control the spread of nuclear weapons somewhat because weapons grade material is not readily available and processing technology to produce it is still somewhat identifiable. But we are clearly losing this battle.

Even more frightening are newer non-nuclear technologies for mass destruction and mass death. Biotechnology has almost no systematic controls on it and it is moving, evolving, and developing at a rate that no technology has experienced in the history of human invention. We are creating new medicines and even new organisms monthly if not weekly. Knowledge of the technologies used to accomplish these wondrous feats is spreading. Further, the equipment and processes used to achieve these new developments are generally available in industrialized nations and are being dispersed rapidly throughout the world. It is unlikely that the free world can construct processes to effectively limit the spread of this knowledge and the related technology.

The potential harm from the miss-use of biotechnology should frighten everyone in this room, in this country, and, in fact, everyone in the world. It is conceivable that one could engineer an organism that targets and kills selective segments of the world population; much of the technology has already been demonstrated. Those who might wish to commit genocide (and there have been many in the history of the world) will be able to create biological weapons that accomplish this dastardly goal without firing a shot. Bio-weapons are the ultimate terrorist weapon in terms of effects. They can kill indiscriminately and cause vast waves of fear across a target population. As new technologies like bioengineering spread, they become available to almost everyone. That means that a wide spectrum of bad actors might conceivably gain access to technology that can be used to kill literally millions. We need to be able to find these bad guys and deal with them before they can develop and use this new technology for evil purposes. It will not matter whether the evildoer is an organic crazy like the Uni-bomber of the 1980's or an organized international terror group like Al Qaeda. We must develop an

intelligence capability to find those who seek to use this technology for evil purposes and to deal with them before they use it.

This is the key part of that last statement – before they use it. Like nuclear weapons, we cannot afford a policy that is designed only to react to a threat once it is demonstrated. We cannot wait until several hundred thousand or millions die from a biological attack to develop and deploy capabilities to find and neutralize the threat. The consequences of first use are far too high. Extreme use of a bio-weapon against the US could render us unable to respond or even function effectively as a nation.

Such extreme power to wipe out entire populations was reserved to only a few super-powers in the twentieth century. In the twenty-first century individuals and small groups could gain access to the power to kill millions. In this century this power will be so available that we must develop 1) the capability to identify those who would use this vast power for harm, 2) the ability to follow the chemical, materials, and processes used to develop bio-weapons, and 3) the ability to react to neutralize threatening activities prior to their use. This new set of intelligence needs and requirements will stretch our abilities and budget as never before. But failure to address these new threats could well bring about our national demise.

Even more daunting is the fact that the biotechnology revolution with all of its benefits and threats is but one of the new sciences that will revolutionize our lives during this century. Rapidly on the heels of the vast developments in biological sciences is the exploding science of neuro-technology. We are beginning to finally understand a lot about how the brain works and how to interface modern technology with it. Today we are developing prostheses that use neuro-signals to activate motors so the prostheses moves like a natural limb. We are developing implants that allow some blind people to see and quadriplegics to control computers and machinery. Along with these developments are discoveries and inventions that allow computers to monitor the alertness of individuals. On the not-too-distant horizon are technologies that will allow us to directly interface computers with the human brain. These technologies will vastly increase the effectiveness of all human beings, for example, giving us far better access to the wealth of data and information that today is resident on the internet. But, we cannot even begin to imagine all the uses of this technology for evil purposes. The ease with which internet viruses are propagated around the world today causing millions of dollars of damage should forewarn us about a time when cyber-warfare might not only attack and spoof our systems, but might also attack and spoof our thinking.

Moving at an equally rapid pace are developments in nano-technology. We are creating a vast capability to manufacture devices at the atomic level. Machines so small they cannot be seen without the assistance of an electron microscope. The potential of these technologies is mind-boggling. We will be able to produce nano sensing, communications, and processing devices that will far outpace anything available today. Technical intelligence requirements as we know them today will change as significantly as word processing did when we went from typewriters to computers. These

technologies have significant potential for good and for harm. Without focused attention the potential for good may not be realized while the potential for evil spreads.

As the Committee knows, we must also pay attention to the dynamics of an increasingly global economy. This is an economy where actions by major players like China, India, and the European Union can significantly affect the well being of the citizens of the US. Without a deep and profound understanding of the dynamics of this new global economy we will not be able to live and prosper in it without risking harm perpetrated against us by those with different and sometimes nefarious agendas.

Similarly, we need to much better understand the dynamics of a new world information infrastructure that drives opinions for or against us in a variety of ways. It is clear that in the current war against terrorism we often fail to win or even understand the war of ideas that underlies much of the hatred behind terror acts. Before we can counter, or even engage effectively in this new world of ubiquitous information and communication, we must understand it, understand who is driving which messages, where the control points and leverage points are, and what tools we have or will need to effect change. Along with understanding the dynamics of world opinion is developing the capability to identify those who are using this capability against us. This type of intelligence collection and analysis is in it infancy and will need focused and long-term attention from Congress to develop properly in the Intelligence Community.

Finally, on the threat side, we need a much greater understanding of the motivating role of radicalism in today's world. How competing concepts for governance, like the desire for an Islamic Caliphate, drive individuals and populations to actively oppose our way of life. Cultural intelligence-the in-depth study of cultures- has been lost in our Intelligence Community for more than a generation. Anthropologists, generally of the 1960's philosophy that the intelligence-military complex is evil, have long been estranged from our national security communities and currently have very little contact with those in the community who need their assistance badly.

During the 1960's and 1970's we invested heavily in academia to create programs and institutes that studied the Soviet model. We studied their language, culture, philosophy, and approach to governance. As a result we produced generation after generation of Soviet and cold-war scholars that staffed intelligence and policy positions in the national security apparatus of the US government. Today, most of the individuals who hold senior positions in our national security establishment (including our current Secretary of State and the National Security Advisor) were trained in this fashion. It is time that we began investing more to create future generations of policymakers who will be versed in emerging issues of cultural intelligence-Islamic radicalism, institutionalized corruption, culture change in the world, global economics, and the spread of technology.

Needed Capabilities

Finding and Tracking Individuals. Today we spend vast sums of money developing and deploying technologies and capabilities that were designed to address the threats posed by nation-states. Since the threats posed by nation-states continues we must continue to invest in these technologies and capabilities for some time to come. But we need to increasingly consider new aggressive investments in capabilities that address the new threats posed by individuals and groups. We must also consider capabilities that allow us to track technology and its use by nation-states, individuals, and groups.

We need far better capabilities to find and track with precision individuals who pose a threat wherever they are hiding in the world's populations, sometimes in our own country. I consider this to be the most pressing new requirement of our intelligence apparatus. We desperately need the capability to identify individuals who wish us and others in the world harm and who are willing to develop and employ weapons of mass destruction to do it.

Even thinking about intelligence as a means to ascertain the motivations of individuals vs. nation-states is new and difficult for many traditional intelligence professionals. In the past we were concerned with the motivations and locations of the leadership of nation-states, but seldom with the prospect of searching through an entire population to identify bad guys. This involves not just new technology but new ways of thinking about intelligence and information. We need an entirely new capability from sensing equipments to analysis to address this need.

This capability to find, identify, and track individuals attempting to gain access to WMD and to use it, must by necessity, be available across the entire world to be effective. If those with nefarious intentions can hide in the US or other populations they will. This raises significant international, civil rights and civil liberties issues that must be addressed up-front and dealt with before we can successfully develop and use these technologies and techniques. But we need to address these issues anyway. Industry is already developing and deploying very sophisticated technologies to identify and track individuals in the general population. The motivation in industry is generally commercial or economic, but we should still be greatly concerned about the effects of this technology on civil liberties. We are already are at the point where life insurance is sometimes denied not based on information provided on the application or acquired through a physical examination, but by the use of health profiles developed through modeling of the buying and eating habits of individuals derived from information acquired from frequent buyer and discount cards.

I am confident that we can develop policies, processes, and technologies that will allow us to use these invasive technologies to find bad guys while ensuring the civil liberties and privacy that are part of our democratic system. The Potomac Institute for Policy Studies currently sponsors a program called Guardian that seeks to bring technologists, civil libertarians, and policy makers to the table to discuss the various aspects of this problem and jointly develop recommendations that satisfy competing objectives.

Avoiding Technological Surprise. We also need to re-vitalize our programs for tracking technology developments around the world. During the 1960's and 70's vast amounts of money were spent by the intelligence community to track technology developments, particularly in the Soviet Union, to prevent a technological surprise that could vastly change the balance of power. These programs have fallen in general disarray. We must rebuild them and direct them in a way that will once again alert us to any potential threat from a technology development that might change our security environment. During the last decade the US Congress more than doubled the amount of money spent on biotechnology in this country, yet today more money is still spent collectively overseas on biotech than is spent in the US. The situation is equally unbalanced in the areas of nano-technology and information technology.

The US leads the world in technology innovation and development, but this is a temporary lead. Developments in most the technologies I have mentioned in this testimony are occurring overseas almost as fast as they are in the US, and given the vast sums being spent on research overseas, its is just a mater of time before other areas of the world will lead in many technologies. We must track these developments with a completeness and precision that will prevent our being surprised by capabilities that exceed our own, or that uniquely threaten the US or world population.

Massive Processing, Modeling, and Automated Analysis. Many of the threats and challenges mentioned above are beyond the ability of any one human to individually understand. We will need a massive computer modeling and analysis capability that can sort through the masses of data that are increasingly available to identify the trends and connections that define the information and knowledge we seek. This type of computer and information technology designed to assist and support analysis, indications, and warning, is not currently envisioned in the intelligence community but is badly needed. Creating this capability is on the order of creating a new National Security Agency. One that has the assets necessary to look at, screen, sort, correlate, analyze, and report on ALL of the data and information available in the open and classified source now and in the future. Today our intelligence community looks at about 1% of the available open source, analyzes about 30% of what it collects through classified sources, and collects an estimated 2-6% of the target environment. (any classification issue here?). Most knowledgeable people today estimate that to address the requirements of finding and tracking key individuals, finding and tracking WMD and related materials, and develop an understanding of the trends in world societies will require a level of persistent surveillance that vastly increases the current amount of collected and analyzed data. There is simply no way we will ever be able to analyze and use the required level of data without computer capabilities that are several orders of magnitude greater than we are employing in the intelligence community today. This technology is not beyond our reach, but it will be expensive to acquire and maintain.

New Sensing Technologies. To adequately track the materials and processes involved in the creation of weapons of mass destruction we will need to develop and deploy new

sensors that are capable of recognizing these materials and process. Much of this technology has already been identified and demonstrated. This technology is generally lumped under the intelligence community heading of MASINT, Measurement and Signatures Intelligence. MASINT has floundered for two decades as a fourth level stepchild of the well-established disciplines of SIGINT, IMINT, and HUMINT. It has suffered from a lack of ownership, lack of sponsorship, and lack of priority. Today we spend billions to maintain and deploy the latest SIGINT and IMINT sensors while proven MASINT capabilities are generally neglected and only deployed when money and space are available.

Yet it is clear that many MASINT technologies can significantly contribute to our ability to find and track WMD. The priority of these technologies as well as their institutional position must be addressed today if we are ever to see their real potential. I would humbly submit that Congress has a very strong role in making this happen in a timely fashion.

Beyond the technologies that we call MASINT today, we need a new and very well funded R&D program to utilize all of the potential of the new sciences (nano, neuro, and material) to address our growing requirements. This R&D program will have to be on the order of several billion dollars (about the size of DARPA) per year to be effective. It will need a personnel and acquisition process approach that maximizes success. The model of DARPA is the best one we have in the US government. Perhaps it is time to consider an Intelligence Community DARPA.

New HUMINT. The affairs of mankind have changed greatly since the advent of human intelligence. Yet our tradecraft has in-fact digressed in technique and capability. During WWII the sine qua non of human intelligence was placing our agents in the enemy's camp. During the cold war, emplacement of US citizens was impractical at best, so we turned to the technique of recruitment of organic agents to do collection for us. The post cold war world requires recruitment, emplaced agents, and tradecraft far more sophisticated to be successful. Cover has a far different meaning in a world blanketed by the internet. HUMINT has more purpose and opportunity than merely the collection and passing on of rumor and inside information.

We need to rethink our entire approach to HUMINT. It is far more than just increasing the numbers of officers deployed overseas. It is the use of our military, police, and diplomatic liaison corp., etc. to collect and often to implant information and technology. Yet the world of HUMINT in our intelligence community has proven to be the most insular of all government bureaucracies. Without continued strong oversight and guidance they will not change.

New Philosophy. Above all, our Intelligence Community needs an embedded philosophy that emphasizes knowledge above data. Our current construction values data. We have built stovepipes to collect, analysis and protect various forms of data unique to

the intelligence community. This worked well in a world where access and control of the data was power. The internet and the information revolution changed all of that in the real world. Today much more data is free and readily available via the internet and digital technology. It will become more accessible as today's internet develops and transforms. What is essential is the ability to correlate that data into useful and unique information and knowledge.

We need to continue to reform our community into one where we value and protect our ability to correlate data into information and knowledge. We can only do this when we break down walls that were constructed to protect and value the data. Let us set data free by ensuring access to it by all elements of the intelligence community. Let all analysts have access to everything relevant to their tasking. Then let us value and protect the unique assessments and correlations that these analysts and analytic tools provide us.

Conclusion. The reforms enacted by this body have already set the stage for the types of change and reform that I have addressed here. But the new law just set the stage. You have provided sound legislation; now we need smart policy and adept capability to truly secure our nation. Achieving those policies and that capability will require continued oversight, legislative and executive branch attention and priority, and significant new investment. Unfortunately, as a nation we have a record of funding certain crucial initiatives only after some great tragedy has focused our attention. With the enormous scale of potential harm from today's and tomorrows emerging threats, we simply cannot wait until after disaster strikes to fund these urgently needed capabilities.

Thank you for the opportunity to express my views. I and the Potomac Institute for Policy Studies stand ready to assist any way we can to make all of this happen.